BAB 2

LANDASAN TEORI

2.1 Teori Umum

2.1.1 Pengertian Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer, *software* dan perangkat jaringan lainnya yang saling bekerjasama untuk mencapai suatu kinerja jaringan yang sama. Jaringan komputer dapat disebut juga himpunan *interkoneksi* sejumlah komputer *autonomous*. Dua buah komputer dikatakan terinterkoneksi bila keduanya dapat saling bertukar informasi.

Agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer meminta dan memberikan layanan (*service*).Pihak yang meminta / menerima layanan disebut klien (*client*) dan yang memberikan / mengirim layanan disebut pelayan (*server*).Arsitektur ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

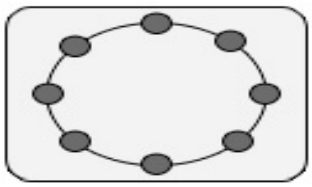
2.1.2 Klasifikasi Jaringan Komputer

Physical Topology adalah gambaran secara fisik dari pola hubungan antara komponen-komponen jaringan, yang meliputi *server, workstation, hub, switch,* pengkabelan, dll. Bentuk umum yang biasa digunakan adalah sebagai berikut :

Ring

Pada topologi ini setiap *node* saling berhubungan dengan *node* lainya sehingga berbentuk seperti lingkaran (*ring*). Metode *token-ring* (sering disebut ring saja) adalah cara menghubungkan komputer sehingga berbentuk *ring* (lingkaran). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai *loop*, data dikirimkan kesetiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan. Terdapat keuntungan dan kerugian dari tipe ini yaitu:

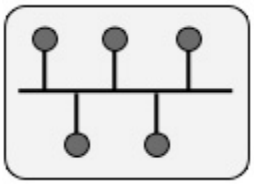
- Keuntungan : Hemat kabel.
- Kerugian : Peka kesalahan, pengembangan jaringan lebih kaku.



Gambar 2.1 Topologi *Ring*

- **Bus**

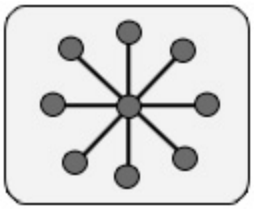
Topologi *bus* disebut juga linear *bus* karena dihubungkan hanya melalui satu kabel yang *linear* seperti terlihat pada gambar 2.2.kabel yang umum digunakan adalah kabel koaksial.



Gambar 2.2 Topologi *Bus*

- **Star**

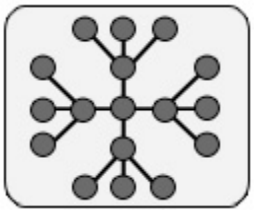
Hubungan antar *node* melalui suatu perangkat yang disebut *hub* atau *concentrator*. Setiap *node* dihubungkan dengan kabel ke *hub*.



Gambar 2.3 Topologi *Star*

- **Extended Star**

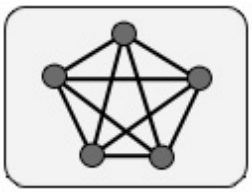
Menggabungkan beberapa topologi *star* menjadi satu topologi. *Hub* atau *Switch* yang digunakan untuk menghubungkan beberapa komputer pada satu jaringan dengan menggunakan topologi *Star* dihubungkan lagi ke *hub* atau *switch* utama.



Gambar 2.4 Topologi *Extended Star*

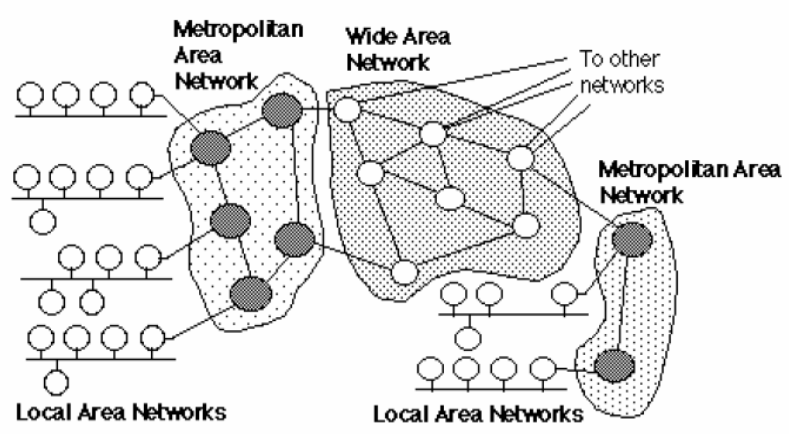
- **Mesh**

Setiap komputer memiliki hubungan langsung dengan semua *host* lainnya dalam jaringan. Topologi ini juga merefleksikan *internet* yang memiliki banyak jalur ke satu titik.



Gambar 2.5 Topologi Mesh

Berdasarkan dari luas area yang dicakup, jaringan komputer terbagimenjadi tiga ukuran, yaitu *Local Area Network* (LAN), *Metropolitan Area Network* (MAN), dan *Wide Area Network* (WAN). Pada gambar 2.6 akan menampilkan cakupan masing – masing area.



Gambar 2.6 Cakupan Daerah Suatu Jaringan

1. LAN

Jaringan yang lingkupnya paling kecil, biasanya mencakup rumah, gedung atau kampus.

2. MAN

Merupakan jaringan yang mencakup sebuah area metropolitan, yaitu sebuah daerah yang lebih besar daripada LAN dalam sebuah area geografis, biasanya terkoneksi dalam satu kota yang jaraknya bisa mencapai 10 km.

3. WAN

Merupakan jaringan yang menghubungkan antar LAN yang mencakup jarak geografis yang sangat luas. Dibandingan LAN, WAN lebih pelan, karena membutuhkan permintaan koneksi ketika ingin mengirim data. WAN beroperasi pada *Layer* 1, 2 dan 3 (khususnya X.25 dan *Integrated Services Digital network* (ISDN)).

2.1.3 Peralatan Jaringan

- ***Router***

  Router berfungsi untuk memisahkan jaringan.Dengan menggunakan*routing protocol, router* dapat menentukan jalur terbaik untukpaket-paketnya. *Router* bekerja pada *Layer*3 pada model OSI (*Network Layer*). *Router*dapat membagi *collision domain*dan *broadcast domain*.

- ***Switch***

  *Switch*adalah alat penghubung jaringan dengan *forwarding* berdasarkan alamat MAC. *Switch* membagi *collision domain* tetapi tidak membagi *broadcast domain*. *Switch*bekerja pada *layer 2*pada model OSI *(Data link Layer)*dan ada juga yang bekerja pada *layer* 3 (*Network layer*) pada model OSI. Perbedaan yang mendasar antara *switch layer* 2 dan *switch layer* 3 adalah kemampuan *switch layer* 3 dapat melakukan proses *routing*.

2.1.4 Konsep *Networking* Model

Tujuan dari OSI Layer adalah :

1. Mengurangi kompleksitas dan mempercepat evolusi dalam dunia jaringan, karena masing – masing dapat fokus hanya pada satu *layer* saja tanpa perlu khawatir dapat mengganggu fungsi dari *layer* yang lain.
2. Menjamin interoperabilitas dan adanya standarisasi untuk berbagai *vendor* (seperti *router* Juniper dengan *router* Cisco, dapat berkomunikasi dengan adanya standarisasi).

3. Membuat perusahaan untuk lebih fokus terhadap salah satu bagian dari ke tujuh layer dibawahnya.

Gambar 2.7 Model OSI Layer

Gambar 2.7 merupakan gambar dari model OSI. Model OSI terdiri dari 7 layer. Layer 7,6,5 disebut dengan *host layer*, maksudnya adalah proses dalam layer itu terjadi pada saat data masih di dalam komputer, sedangkan *layer* 4,3,2,1 disebut dengan *media layer*. Berikut penjelasan mengenai ke-7 layer tersebut : (**http://cnap.binus.ac.id/ccna/**)

1. *Application Layer* (*Layer* 7)

   Tugas dari *layer* ini adalah menyiapkan komunikasi *end-to-end*. Berperan sebagai *interface* (yang menghubungkan antara manusia dengan komputer). Protokol yang bekerja pada *layer* 7 adalah :HTTP, FTP, SMTP, Telnet, SNMP.

2. *Presentation Layer* (Layer 6)

Layer ini bertugas untuk mendefinisikan *format data*, menampilkan data dan menangani kompresi dan enkripsi. Format data yang bekerja pada *layer* 6 adalah : ASCII, JPEG, GIF, MPEG, WAV, MIDI.

3. *Session Layer* (*Layer* 5)

   Tugas dari *layer* ini adalah :

   - Memulai dan mengakhiri suatu sesi antar dua *end sistem*.
   - Menjaga agar dua aplikasi atau lebih dapat berjalan secara bersamaan.
   - Menjaga sesi agar tetap terpisah, sehingga tidak saling tumpah tindih

4. *Transport Layer* (*Layer* 4)

   Tugas dari layer ini adalah :

   - Memikirkan bagaimana data dapat terkirim secara:

   1. *Reliable* (dapat dipercaya)

      Mengutamakan pengiriman secara akurat.Contoh :*browsing*, *email.*

   2. *Unreliable*

      Mengutamakan kecepatan dalam mengirim data.Contoh : VoIP, *video streaming*.

      - Dapat membuat dan menjelaskan layanan yang digunakan dengan melihat nomor *port*. Contoh : bila menggunakan port 80, artinya sedang melakukan *browsing*.
      - Pada *layer* ini terjadi proses segmentasi (memecah data menjadi ukuran yang lebih kecil) dan juga proses *reassemble* (penyusunan kembali, data yang telah dipecah). Protokol yang bekerja pada *layer* 4 adalah : TCP, UDP.

5. *Network Layer* (*Layer* 3)

   Layer ini berfungsi untuk mendefinisikan alamat-alamat IP , membuat *header* untuk paket-paket, dan mencari jalur terbaik lalu kemudian melakukan *routing* melalui *internetworking* dengan menggunakan *router* dan *switch Layer-3*. Protokol yang bekerja pada *layer* 3 adalah : IP, IPX, AppleTalk.

6. *Data Link Layer* (*Layer* 2)

   Layer ini mendefinisikan bagaimana untuk mengirimkan data melalui suatu media, baik media kabel maupun nirkabel dengan *physical addressing.* Tugas utama dari layer ini adalah *error checking, flow control, Media Acces Control*untuk mengatur paket yang akan berjalan. Protokol yang bekerja pada *layer* 2 adalah : PPP, HDLC, Frame Relay, Ethernet, ATM.

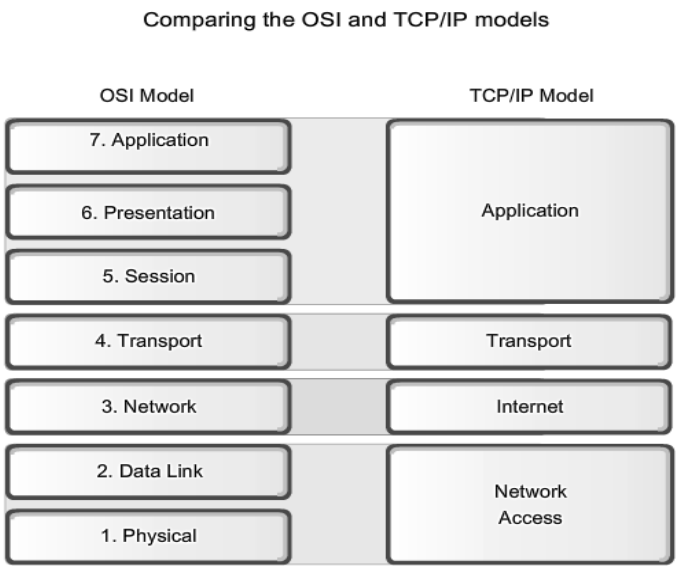
7. *Physical Layer* (Layer 1)

   Layer ini berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya *Ethernet* atau *Token Ring*), danpengkabelan. Selain itu, level ini jugamendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio**.**Protokol yang bekerja pada *layer* 1 adalah : Ethernet, V.35, RS-232.

2.1.5 Model *TCP/IP*

Model Referensi *Transmission Control Protocol/Internet Protocol* (TCP/IP) diciptakan oleh Departemen Pertahanan Amerika (DARPA) karena mereka menginginkan jaringan yang dapat bertahan dalam kondisi apapun,

sekalipun perang nuklir.*Department of Defense* (DOD)menginginkan jaringan yang dapat mengirimkan paket pada setiap saat, dalam kondisi apapun, dari satu titik ke titik lainnya. Dari keinginan tersebut lahirlah model *TCP/IP*, dimana menjadi standar pertumbuhan internet. Model *TCP/IP* Memiliki 4 *layer*: *LayerApplication,LayerTransport, Layer Internet,* dan *LayerNetwork Access*. Penting untuk diperhatikan bahwa beberapa *layer* pada Model *TCP/IP* memiliki nama yang sama dengan *layer* pada Model OSI.



Gambar 2.8 Model TCP/IP *Layer*

(Sumber :**http://cnap.binus.ac.id/ccna/**)

1. ***Layer Application***adalah sebuah aplikasi yang mengirimkan data ke transport *Layer*. Misalnya FTP, *emailprograms* dan *webbrowsers*.
2. ***Layer Transpor****t* bertanggung jawab untuk komunikasi antara aplikasi. *Layer* ini mengatur aliran informasi dan mungkin menyediakan

pemeriksaan *error*. Data dibagi kedalam beberapa paket yang dikirim ke internet *Layer* dengan sebuah *header*. *Header* mengandung alamat tujuan, alamat sumber dan *checksum*. *Checksum* diperiksa oleh mesin penerima untuk melihat apakah paket tersebut ada yang hilang pada rute.

3. ***Layer Internetwork***bertanggung jawab untuk komunikasi antara mesin. *Layer* ini meng-enkapsulasipaket dari *TransportLayer* ke dalam *IP datagrams* dan menggunakan algoritma *routing* untuk menentukan kemana *datagram* harus dikirim. Masuknya *datagram* diproses dan diperiksa kesahannya sebelum melewatinya pada *Transport Layer*.
4. ***Layer Networks* Interface** adalah *level* yang paling bawah dari susunan TCP/IP. *Layer* ini adalah *devicedriver* yang memungkinkan *datagramIP* dikirim ke atau dari *phisycalnetwork*. Jaringan dapaat berupa sebuah kabel, *Ethernet, framerelay, Tokenring*, ISDN, ATM jaringan, radio, satelit atau alat lain yang dapat mentransfer data dari sistem ke sistem. *Layernetwork interface* adalah abstraksi yang memudahkan komunikasi antara *multitude arsitektur network*.

2.1.6 Protokol *TCP/IP*

Saat ini, *Internet* dan *World Wide Web* (WWW) adalah istilah yang umum bagi jutaan orang diseluruh dunia. Banyak orang bergantung pada aplikasi–aplikasi yang harus terkoneksi dengan *internet,* seperti surat elektronik dan website. Protokol *Transmission Control Protocol / Internet Protocol* (*TCP/IP*) merupakan mesin dari *internet* dan jaringan diseluruh dunia.Karena

simpel dan berkemampuan tinggi, *TCP/IP* terpilih menjadi satu–satunya protokol jaringan yang berada di dunia saat ini.

TCP dan *IP* dibangun oleh *Department of Defense* (*DOD*) untuk menghubungkan jaringan komputer yang dibuat oleh vendor berbeda kedalam sebuah jaringan (*Internet*). Hal tersebut awalnya berhasil karena hanya mengirimkan beberapa layanan dasar seperti : pengiriman *file,* surat elektronik dan *remote login* yang melewati banyak *client* dan *server*.IP menyediakan routing dari sebuah departemen ke jaringan perusahaan, lalu ke jaringan regional dan berakhir di global *internet.*

Pada zaman komunikasi saat ini, sebuah jaringan harus tahan dari sebuah kerusakan.Oleh karena itu, *DOD* mendesain *TCP/IP* secara handal dan secara otomatis memperbaiki apabila ada kegagalan dari suatu node.Dengan desain seperti itu, cocok untuk diterapkan pada jaringan yang sangat besar dengan sedikit pengaturan terpusat.

TCP didefinisikan dalam RFC 793.*TCP* mempercayai *IP* untuk pengiriman data *end-to-end* termasuk masalah routing. *TCP* menjamin transmisi dan aliran data dari asal ke tujuan.

Karakteristik yang terdapat pada protokol *TCP* :

1. *Reliability*

   TCP menyediakan pengiriman data yang dapat diandalkan. Untuk dapat diandalkan, *TCP* menggunakan *field Sequence* dan *Acknowledgment* yang terdapat pada *header TCP*. Bila terdapat *TCPsegment* yang rusak maka *segment* yang rusak tersebut akan dikirim ulang.

2. *Flow Control*

Untuk mencegah data terlalu banyak dikirim dalam satu waktu, maka dilakukan *flow control* dengan *windowing.TCP* memanfaatkan *field Sequence* dan *Acknowledgment* dan *window* yang terdapat pada *header TCP*. Ukuran dari window berubah – ubah setiap waktu.Window awalnya berukuran kecil lalu kemudian membesar hingga terjadi *error*.

3. *Connection – oriented*

   Sebelum data dapat dikirim, terlebih dahulu melakukan pertukaran informasi antar dua *host.*

4. *Data Segmentation*

   TCP membagi data menjadi ukuran yang lebih kecil dan tidak lebih dari ukuran *maximum transmission unit* (MTU). Pada sisi penerima *TCP*akan melakukan *reassembly* ketika menerima *segment* dan juga dapat mengurutkan kembali *segment – segment* yang datang tidak berurutan.

Layanan layer network yang diimplementasikan pada protokol *TCP/IP* adalah Internet Protokol (*IP*). *IP* versi 4 saat ini yang paling umum digunakan.*IP* versi 6 diciptakan dan telah diimplementasikan di beberapa tempat, umumnya di *Internet Service Provider*.*IP* dirancang sebagai protokol dengan tingkat *overhead* yang rendah, *IP* hanya menyediakan fungsi pengiriman paket dari sumber ke tujuan melalui sistem jaringan yang saling terhubung.*IP* tidak dirancang untuk mengatur aliran paket. Adapun karakteristik dasar dari *IP* versi 4 adalah :

1. *Connectionless*

   Paket *IP* dikirim tanpa memberitahu terlebih dahulu penerima bahwa paket tersebut akan datang. Oleh karena itu, *IP* tidak memerlukan pertukaran

informasi dahulu sebelum *IP* dapat mengirim paket.Sehingga didalam header PDU tidak perlu ada penambahan *field*. Proses tersebut mengurangi terjadinya *overhead* pada *IP*.

Pengiriman paket bersifat *connectionless* berdampak pada tidak berurutnya paket yang diterima ditujuan. Bila hal tersebut terjadi, layanan pada layer diatasnya (*TCP*) yang akan memecahkan masalah tersebut.

2. *Best-Effort (Unreliable)*

Protokol *IP* tidak menyediakan layanan yang *reliable*.Bila dibandingkan dengan protokol yang *reliable*, maka header *IP* berukuran lebih kecil.Mengirimkan paket yang berukuran kecil berdampak kecilnya overhead yang terjadi.*Overhead* yang kecil menyebabkan kecilnya terjadi delay dalam pengiriman.

Maksud *reliable* disini bukan berarti *IP* bekerja pada suatu saat, namun tidak bekerja sebagaimana mestinya pada saat yang lain. *Unreliable* disini berarti *IP* tidak memiliki kemampuan untuk mengatur, dan memperbaiki paket yang rusak maupun paket yang tidak terkirim.

3. *Media Independent*

IP versi 4 dan *IP* versi 6 tidak bergantung pada media yang digunakan, IP dapat berkomunikasi pada media kabel, fiber optik maupun sinyal radio. Terdapat karakteristik yang oleh layer *network* perhatikan yaitu ukuran maksimum dari PDU yang tiap media dapat kirimkan.Karakteristik tersebut dikenal sebagai *Maximum Transmission Unit* (MTU). Bagian dari pengaturan komunikasi antara layer *Data Link* dan layer *Network*. Layer *Data Link* melewatkan MTU naik ke layer *Network* dan menentukan

seberapa besar ukuran pembuatan paket. Pada beberapa kasus, *intermediary device* seperti *router*akan membagi paket ketika akan dikirim dari satu media ke media lain dengan ukuran MTU yang lebih rendah. Proses itu disebut dengan istilah *fragmentation.*

2.1.7 Pengalamatan *IP*

Internet terdiri dari jutaan *host* dan dimana masing – masing diidentifikasi secara unik oleh pengalamatan pada layer *Network*. Untuk berharap setiap *host* dapat mengetahui alamat dari *host* yang lain dapat menyebabkan performa dari peralatan jaringan yang dapat menurun. Membagi jaringan besar menjadi kumpulan grup yang lebih kecil dapat mengurangi *overhead* yang tidak perlu.

Untuk dapat membagi suatu jaringan, diperlukan pengalamatan yang terstruktur (hirarki), yang juga digunakan untu komunikasi data antar jaringan melalui internetwork.

IP versi 4 memiliki pengalamatan terstruktur, terdiri dari 32 bit yang ditulis dalam nilai – nilai desimal 4. Desimal tersebut terdiri dari 1 byte atau 8 bit.Setiap desimal dalam alamat *IP* disebut juga sebagai oktet.*IP* versi 4 didefinisikan pada RFC 791, dimana dijelaskan juga pembagian kedalam kelas – kelas. Alamat IP terdiri dari dua bagian yaitu *network* ID dan *host* ID. Dimana *network* ID menentukan alamat jaringan dan *host* ID menentukan alamat *host* atau komputer. Untuk menentukan alamat kelas IP, dilakukan dengan memeriksa 4 bit pertama (bit yang paling kiri) dari alamat IP. (dapat dilihat pada table 2.1)

Tabel 2.1 Alamat Kelas IP

Kelas	Alamat *Bit* Pertama	Desimal
A	0xxx	1-126
B	10xx	128-191
C	110x	192-223
D	1110	224-239
E	1111	240-254

1. Kelas A

Bit pertama alamat IP kelas A adalah 0, *network* ID 8 bit dan panjang *host* ID 24 bit. Kelas A digunakan untuk jaringan yang berskala besar, terdapat 126 jaringan dan tiap jaringan dapat menampung hingga 16 juta *host*. Alamat IP kelas A dimulai dari 1.0.0.0 sampai dengan 126.255.255.255. Alamat oktet awal 127 tidak boleh digunakan karena digunakan untuk mekanisme *Inter-process Communication* di dalam perangkat jaringan yang bersangkutan.

2. Kelas B

Dua bit awal dari kelas B selalu diset 10 sehingga *byte* pertama kelas B bernilai antara 128 – 191. *Network* ID adalah 16 bit pertama dan *host* ID 16 bit sisanya. Kelas B digunakan untuk jaringan berskala menengah hingga besar, terdapat 16.384 jaringan dan tiap jaringan dapat menampung

sepenulisr 65 ribu *host*.Alamat kelas B dimulai dari 128.0.0.0 sampai dengan 192.167.255.255.

3. Kelas C

Tiga bit awal dari kelas C selalu diset 111, sehingga *byte* pertama kelas C bernilai antara 192 – 223. *Network* ID adalah 24 bit dan *host* ID 8 bit sisanya. Kelas C biasa digunakan untuk jaringan kecil, terdapat 2.097.152 jaringan dan tiap jaringan dapat menampung 256 *host*.Alamat kelas C dimulai dari 192.168.0.0 sampai dengan 223.255.255.255.

4. Kelas D

Empat bit awal dari kelas D selalu diset 1110, sehingga *byte* pertama kelas D bernilai antara 224 - 239. Kelas D digunakan untuk keperluan multicast, yaitu suatu metode pengiriman yang digunakan bila suatu *host* ingin berkomunikasi dengan beberapa *host* sekaligus, dengan hanya mengirim satu datagram saja.Alamatdari kelas D adalah 224.0.0.0 sampai dengan 239.255.255.255.Alokasi alamat tersebut ditujukan untuk keperluan sebuah grup, bukan untuk *host* seperti pada kelas A, B dan C.

5. Kelas E

Empat bit awal dari kelas E selalu diset 1111, sehingga *byte* pertama kelas E bernilai antara 240 – 254. Kelas E digunakan sebagai kelas eksperimental yang disiapkan untuk keperluan di masa mendatang.

2.1.8 Private dan Publik IP Address

Macam – macam *IP Address* :

1. *Private* IP address

Hampir seluruh alamat pada IPv4 merupakan alamat publik yang dapat digunakan pada jaringan internet, namun terdapat juga blok alamat yang digunakan untuk keperluan terbatas atau tidak terhubung dengan internet. Alamat tersebut disebut sebagai alamat *Private.*

Blok alamat *private* adalah :

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Host - *host* yang tidak memerlukan akses ke internet dapat menggunakan alamat *private* sebanyak apapun. Namun, jaringan internal tetap harus didesain dengan pengalamatan yang baik dan terstruktur sehingga alamat yang digunakan tetap unik untuk network internal tersebut.

Host yang berada di jaringan yang berbeda dapat menggunakan alamat *private* yang sama. Paket yang menggunakan alamat tersebut sebagai *souce* dan *destination* tidak akan muncul di jaringan internet. *Router* atau firewall yang terletak di ujung jaringan tersebut harus memblok atau menterjemahkan alamat – alamat tersebut.

2. Publik Address

Umumnya alamat IPv4 merupakan alamat publik. Alamat tersebut didesain untuk digunakan pada *host* yang dapat diakses oleh *host* lain melalui internet.

2.1.9 Routing

Pada saat pengiriman paket, paket tersebut dapat melewati jaringan yang berbeda.*Intermediary device,* seperti *router* adalah perangkat jaringan yang digunakan untuk menghubungkan antara jaringan tersebut. Selain itu, peran dari *router* adalah untuk memilih jalur terbaik dan membawa paket ke tujuan, proses tersebut disebut dengan *routing*.**(http://cnap.binus.ac.id/ccna/)**

Pada proses *routing* yang melalui jaringan yang berbeda, paket tersebut akan melewati beberapa *intermediary device.* Setiap perangkat atau *device* yang dilalui paket untuk dapat sampai ke tujuan disebut dengan *hop*.

Router memiliki *routing table,* yang berisi :

1. Daftar jaringan yang terhubung langsung dengan *router* tersebut (*directly connected network*).
2. Jalur menuju jaringan yang tidak terhubung langsung dengan *router* tersebut (*remote network*).
3. Alamat *default route* (0.0.0.0).

Routing terbagi dengan dua cara, yaitu :

1. *Static Route*

Static route digunakan dalam sebuah jaringan yang hanya terdiri dari beberapa *router* saja atau dipakai untuk jaringan kecil dan jaringan yang terhubung ke internet hanya melalui satu *Internetservice provider*.Digunakan *static route* karena hanya *Internetservice provider* tersebut yang menjadi jalan keluar untuk akses ke internet.

Dalam *static route,* pengisian dan pemeliharaan *routing table* dilakukan secara manual oleh administrator. Kelebihan dalam *static* route yaitu tidak memerlukan *bandwith* jaringan yang besar akan tetapi jika salah satu jalur routing-nya terputus maka router tidak bisa mencari alternative jalan baru untuk meneruskan paket data yang dikirim.

2. *Dynamic Route*

Dynamic Route mempelajari rute sendiri yang terbaik yang akan ditempuhnya untuk meneruskan paket dari sebuah jaringan ke jaringan lainnya. Administrator tidak menentukan rute yang harus ditempuh oleh paket-paket tersebut. Administrator hanya menentukan bagaimana cara*router* mempelajari paket dan kemudian router mempelajarinya sendiri. Rute pada *dynamicrouting* berubah sesuai dengan informasi yang didapatkan oleh *router*.

Dynamic route ini digunakan apabila jaringan memiliki lebih dari satu kemungkinan rute untuk tujuan yang sama. Sebuah *dynamic routing* dibangun berdasarkan informasi yang dikumpulkan oleh *routing protocol*.Protokol ini didesain untuk mendistribusikan informasi secara dinamis yang mengikuti perubahan kondisi jaringan.*Routing protocol*

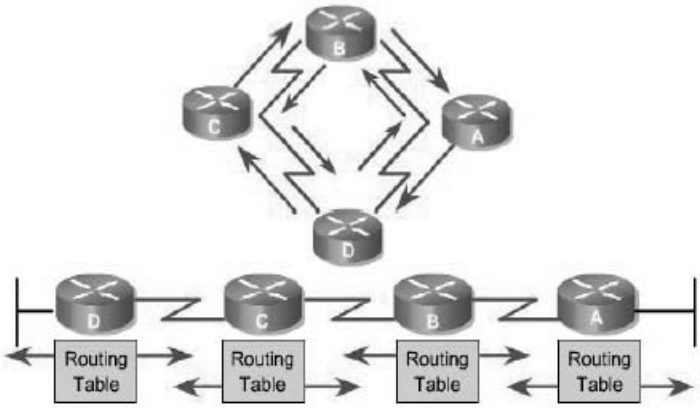
mengatasi situasi *routing* yang kompleks secara cepat dan akurat.*Routing protocol* dirancang tidak hanya untuk mengubah ke rute backup bila rute utama putus, namun juga dirancang untuk menentukan rute mana yang terbaik untuk mencapai tujuan tersebut.

Pengisian dan pemeliharaan *routing table* tidak dilakukan secara manual oleh administrator.Router saling bertukar informasi agar dapat mengetahui alamat tujuan dan menerima *routing table*.Pemeliharaan jalur dilakukan berdasarkan pada jarak terpendek antara perangkat pengirim dan perangkat tujuan.

Dynamic routing protocol terdiri dari beberapa kategori, yaitu :

1. *Distance Vector Route Protocol* (DVRP)

   Routing protocol ini hanya tahu mengenai jarak dan arah. Jarak yang dimaksud dengan jumlah dari *hop count*, sedangkan arah merupakan *next hop router* atau *exit interface*.Contoh *distance vector* adalah *Routing Information Protocol* (RIP) *version* 1, RIP *version* 2, *Interior Gateway Routing Protocol* (IGRP), *Enhanced Interior Gateway Routing Protocol* (*EIGRP*).



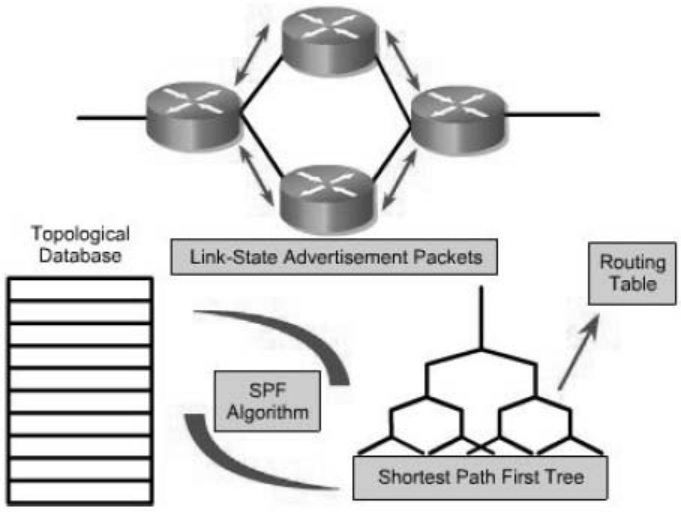
Gambar 2.9 Konsep *Distance Vektor*

(Sumber :**http://cnap.binus.ac.id/ccna/**)

2. *Link State Routing Protocol* (LSRP)

Routing protocol ini lebih *modern* dibanding *distancevector*.Algoritma pada *Link State Routing Protocol* ini menghitung dan menggunakan jalan yang terpendek ke *router* lain. Kelebihan *routing protocol* jenis ini adalah informasi akan di*update* dikirim jika ada perubahan topologi jaringan, lebih cepat untuk konvergen, tidak rentan terhadap *routing loop*, dan lebih sedikit menghabiskan *bandwidth* dibanding *distance vector*, kelemahannya antara lain lebih sulit untuk dikonfigurasi dan membutuhkan lebih banyak memori dan *processing power*mengambil pandangan umum seluruh topologi jaringan.

Contoh *Link State Routing Protocol* adalah *OSPF* dan IS-IS.



Gambar 2.10 Konsep *Link-State*

(Sumber :**http://cnap.binus.ac.id/ccna/**)

3. *Hybrid Routing Protocol*

Hybrid routing protocol adalah merupakan kombinasi dari *distance vector* dan *link-state routing protocol*, dimana bekerja dengan cara berbagi informasi mengenai seluruh jaringan dengan *router* tetangga. *Hybrid routing protocol* ini hadir setelah Cisco Sistem membuat *routingprotocolEIGRP* (*Enhanced Interior Gateway Routing Protocol*) yang merupakan pengembangan dari IGRP klasik yang bersifat *openstandart*. *EIGRP* dari Cisco ini bersifat *proprietary*, dengan kata lain hanya dapat digunakan oleh perangkat jaringan buatan Cisco.**(http://cnap.binus.ac.id/ccna/)**

2.1.10 Routing Protocol

- *Routing Information Protocol* (RIP)

Routing Information Protocol(RIP) adalah *routingprotocol* yang mencari jalur terbaik menggunakan *hop count* sebagai *metric.* Jumlah maksimal hop yang diperbolehkan adalah 15, bila mencapai *hop* ke-16 maka akan terjadi *destination unreachable.* Secara *default* periode *update* dilakukan secara *broadcast* atau *multicast* setiap 30 detik. **(http://cnap.binus.ac.id/ccna/)**

RIP memiliki 3 versi yaitu RIPv1, RIPv2, dan RIPng

1. RIPv1

   RIPv1 menggunakan *classfull routing*, tidak mendukung *subnetting* dan tidak mendukung *Variable Length Subnet Mark* (VLSM). Penyebaran informasi RIPv1 secara *broadcast.* RIPv1 didefinisikan pada RFC 1058

2. RIPv2

   RIPv2 hadir sepenulisr tahun 1994 yang mampu menggunakan *classless inter-domain* routing.RIPv2 mendukung VLSM, *subnetting,* dan authentikasi.Penyebaran informasi RIPv2 secara *multicast.* RIPv2 didefinisikan pada RFC 2453

3. RIPng

   RIPng merupakan protokol RIP untuk IPv6.RIPng didefinisikan pada RFC 2080.

- *Interior Gateway Routing Protocol (*IGRP*)*

  *Interior Gateway Routing Protocol (*IGRP*)* adalah protokol yang diciptakan untuk mengatasi kekurangan RIP. *Metric*-nya berupa gabungan

bandwith, delay dan *load.Routing update* yang dilakukan IGRP secara *broadcast* dan tiap 90 detik. Jumlah maksimal hop yang diperbolehkan adalah 255.

IGRP telah mengatasi beberapa kekurangan dari RIP, tetapi IGRP tidak mendukung VLSM. Maka dari itu, Cisco telah membuat *EIGRP* untuk memperbaiki masalah ini.**(http://cnap.binus.ac.id/ccna/)**

- *Enhanced Interior Gateway Routing Protocol* (*EIGRP*)

Enhanced Interior Gateway Routing Protocol (*EIGRP*) adalah protokol dengan optimalisasi untuk meminimalkan ketidakstabilan *routing* yang terjadi setelah perubahan topologi, serta penggunaan dan pengolahan daya *bandwith* pada router.*EIGRP* menggunakan algoritma *Diffusing Update Algorithm* (DUAL) untuk mencari jalur terbaik.

Di dalam *EIGRP* tidak ada *periodic update*, tetapi menggunakan *trigerred update*, yaitu waktu untuk melakukan update *routing table* saat ada perubahan topologi (ketika ada jalur yang putus atau memang ada perubahan topologi). Jumlah maksimal hop yang diperbolehkan adalah 255.

EIGRP merupakan *proprietary* Cisco yang merupakan kelemahan dari *EIGRP* karena hanya berjalan pada *vendor* Cisco saja, tidak bisa dari *vendor* yang lain. *EIGRP* menggunakan beberapa istilah, yaitu :

1. *Successor*

   Istilah yang digunakan untuk jalur terbaik berdasarkan *metric*..

2. *Feasible Successor*

Istilah yang digunakan untuk jalur yang akan digunakan untuk *backup route.*

3. *Neighbor table*

   Istilah yang digunakan untuk tabel yang berisi alamat dan *interface* untuk mengakses ke *router* sebelah atau *directly connected.*

3. *Topology table*

   Istilah yang digunakan untuk tabel yang berisi semua tujuan dari *router* sepenulisrnya.

4. *Reliable transport protocol* (RTP)

   Protokol yang digunakan *EIGRP* untuk mengirim dan menerima paket.

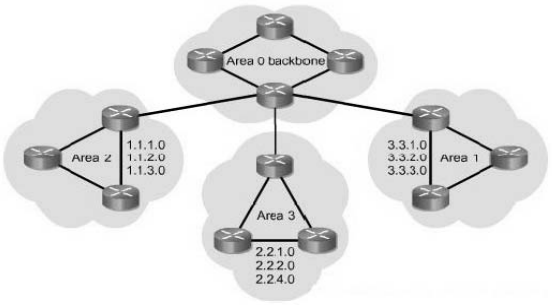
- *Open Shortest-Path First* (*OSPF*)

  Open Shortest-Path First (*OSPF*) merupakan jenis *link state routing protocol* yang melakukan perhitungan jalur terpendek menggunakan *bandwith*(http://cnap.binus.ac.id/ccna/).

  Tipe Paket *OSPF* :

  1. *Hello packet* – Paket hello digunakan untuk membangun dan memelihara *adjacency* dengan *routerOSPF* lainnya.
  2. DBD – *DatabaseDescription* (DBD) berisi daftar-daftar dari *databaselinkstaterouter* pengirim dan digunakan oleh *router* penerima untuk memeriksa dan dibandingkan dengan *databaselinkstatelocal.*
  3. LSR – *ReceivingRouters* kemudian bisa meminta informasi lebih lanjut tentang isi di dalam DBD dengan mengirim *Link-StateRequest* (LSR)

4. LSU – *LinkStateUpdate* (LSU) paket digunakan untuk me-*reply* ke LSRs serta mengumumkan informasi baru. LSUs berisi tujuh jenis *Link-StateAdvertisements* (LSAs) yang berbeda.
5. LSAck – Ketika sebuah LSU diterima, *router* mengirim sebuah *Link-stateAcknowledgement* (LSAck) sebagai konfirmasi penerimaan LSU.

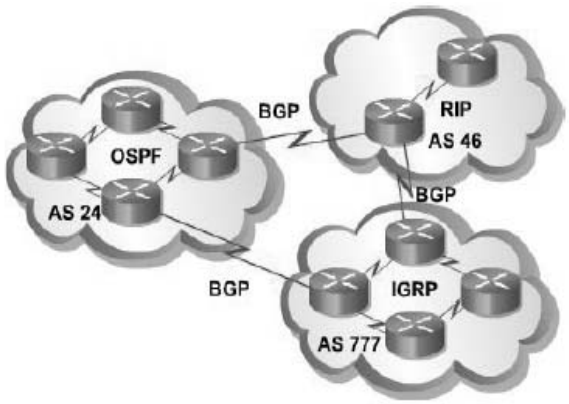


Gambar 2.11 Area Pada *OSPF*

(Sumber :**http://cnap.binus.ac.id/ccna/**)

- *Border Gateway Protocol* (*BGP*)

Border Gateway Protocol atau lebih familiar dikenal dengan nama***BGP*** merupakan sebuah protokol *routinginter-AutonomousSistem*. Fungsi utama sistem *BGP* adalah untuk bertukar informasi *network* yang dapat 'dijangkau' (*reachability*) oleh sistem *BGP*lain, termasuk di dalamnya informasi-informasi yang terdapat dalam list *autonomoussistem* (AS). *BGP* berjalan melalui sebuah protokol *transport*, yaitu TCP.



Gambar 2.12 *BGP*

(Sumber :**http://cnap.binus.ac.id/ccna/**)

2.2 Teori Khusus

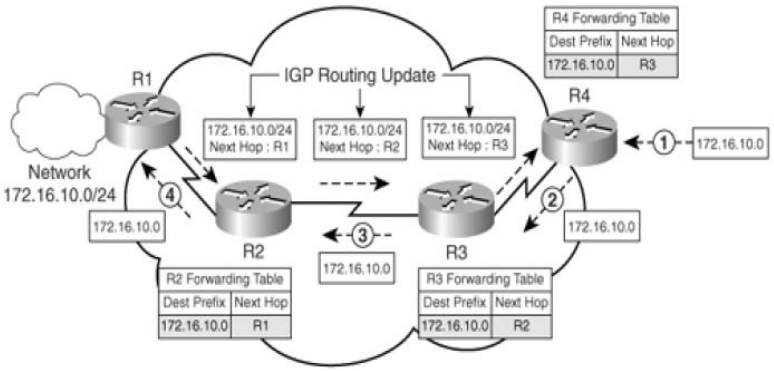
2.2.1 Multiprotocol Label Switching (*MPLS*)

Menurut *Cisco Sistems Learning*(2006), *Multiprotocol Label Switching* (*MPLS*) adalah sebuah metode dengan performa tinggi untuk meneruskan paket melewati suatu jaringan. *MPLS* mengizinkan *router* yang berada di *edge network* untuk menyisipkan label yang simple kedalam sebuah paket. Praktek ini mengizinkan perangkat *MPLS* (ATM *switch* maupun *router* yang ada di tengah *Internetservice provider core*) untuk menyisipkan label di setiap paket.*MPLS* bekerja pada layer 2,5 ini dikarenakan *MPLS* mempunyai keunggulan switching pada layer 2, serta keunggulan *routing* dan skalabilitas pada layer 3.

2.2.2 *Packet Forwarding* pada jaringan IP Tradisional Versus *MPLS*

Pada jaringan IP tradisional, *routing protocol* digunakan untuk mendistribusikan informasi *routing* di Layer 3. Proses penerusan paket dilakukan

berdasarkan alamat tujuan, ketika sebuah paket diterima suatu *router*, maka *router* tersebutakan menentukan *next-hop address* menggunakan alamat IP tujuan dengan informasi yang terdapat pada tabel *routing*. Proses ini akan terus berulang pada tiap *hop* (*router*) dari sumber ke tujuan.



Gambar 2.13 Operasi IP *Forwarding* Tradisional

(http://www.cisco.com/en/US/products/ps6557/prod_presentation_list.html)

Berdasarkan Gambar 2.13 proses penerusan paket adalah sebagai berikut:

1. R4 menerima sebuah paket data yang ditujukan untuk jaringan 172.16.10.0
2. R4 mencari rute untuk jaringan 172.16.10.0 pada label routing dan paket diteruskan ke *next-hop*, *router* R3.
3. R3 menerima paket data tersebut dengan tujuan 172.16.10.0 lalu mencari rute untuk jaringan 172.16.10.0 dan kemudian meneruskannya ke *router* R2.

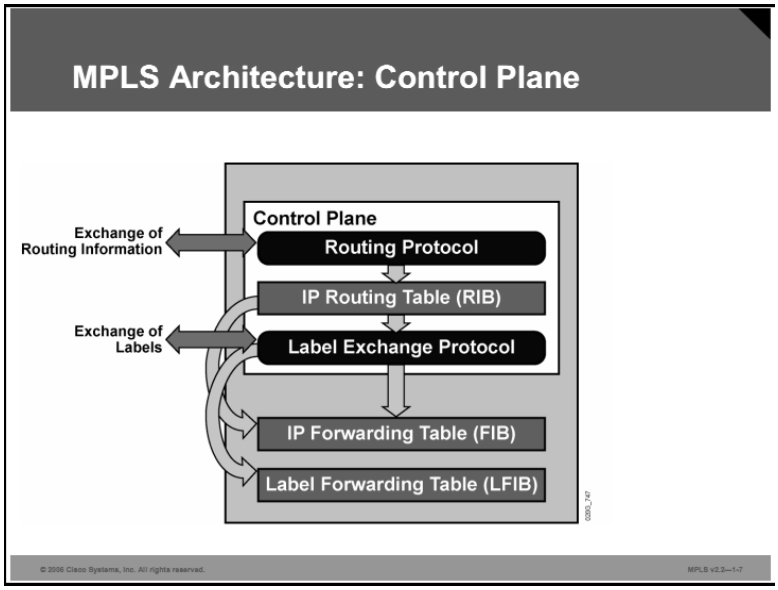
4. R2 menerima paket data tersebut dengan tujuan 172.16.10.0 lalu mencari rute untuk jaringan 172.16.10.0 dan meneruskannya ke *router* R1.
5. Karena router Rl terhubung langsung ke jaringan 172.16.10.0, Rl akan meneruskan paket tersebut ke *interface* yang tepat.

Sedangkan pada jaringan *MPLS*, paket data diteruskan berdasarkan label. Label mungkin akan disesuaikan dengan alamat IP tujuan atau dengan parameter lainnya, misalnya kelas-kelas QoS dan alamat sumber.

2.2.3 Arsitektur *MPLS*

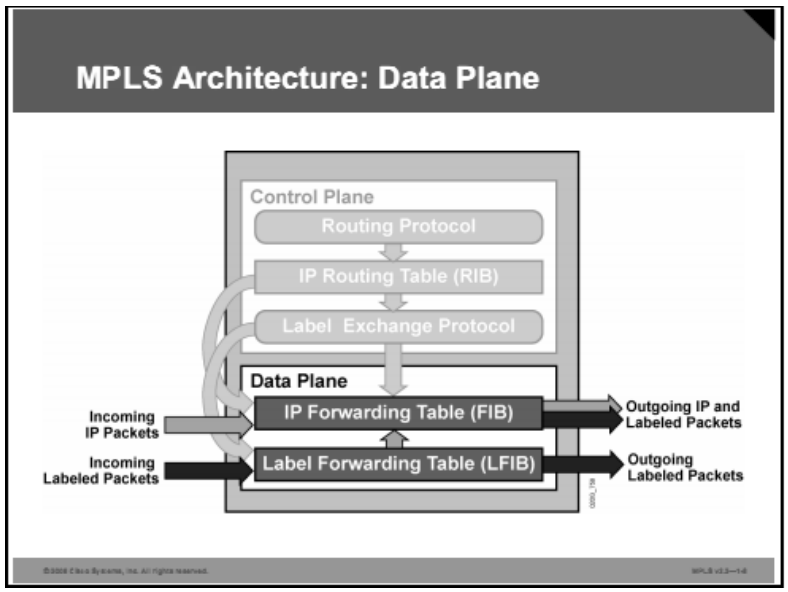
Menurut *Cisco Sistem Learning*(2006), Fungsionalitas *MPLS* dibagi menjadi dua bagian utama blok arsitektur, yaitu:

1. *Control Plane* – menjaga pertukaran informasi *routing* dan pertukaran label diantara perangkat jaringan. C*ontrol plane* membangun *routing table(Routing Information Base[RIB])* berdasarkan *routing protocol* untuk pengaturan *routing* di layer 3. Contoh fungsi *control plane* adalah pertukaran informasi protokol *routing*, seperti *OSPF* dan *BGP*. Selain itu, semua fungsi yang berhubungan dengan pertukaran label antar *router-router* tetangga.



Gambar 2.14 Arsitektur *Control Plane*

2. *Data Plane* - bertugas untuk menjaga penerusan paket-paket data berdasarkan suatu tujuan alamat IP atau label. *Data plane* disebut juga *forwarding plane*. *Data plane* adalah penerus paket sederhana dimana hanya meneruskan suatu tipe dari *routing* protokol atau pertukaran protokol label yang akan digunakan. *Data plane* mengirimkan paket ke *interface* yang tepat berdasarkan informasi yang berasal dari tabel LFIB atau FIB.



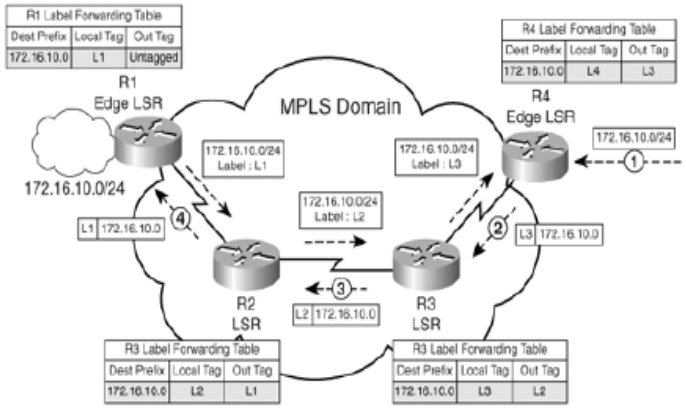
Gambar 2.15 Arsitektur Data Plane

2.2.4 Istilah-Istilah Dalam *MPLS*

Menurut Cisco Sistem Learning(2006), Beberapa istilah penting dalam *MPLS* yang akan digunakan terus dalam skripsi ini, yaitu :

1. *Forwarding Equivalent Class* (FEC) - merupakan sekumpulan paket-paket yang akan mendapatkan perlakuan *forwarding* yang sama (melewati jalur yang sama).
2. *MPLSLabel Switch Router* (LSR) - bertugas dalam *label switching*; LSR menerima *labeled packet* dan menukar *label* tersebut dengan *outgoing label* dan meneruskan *labeled packet* baru tersebut dari *interface* yang tepat. Berdasarkan lokasinya dalam *domainMPLS*, LSR bisa bertugas dalam *label imposition* (addition, disebut juga push) atau pun *label disposition* (removal, disebut juga pop).

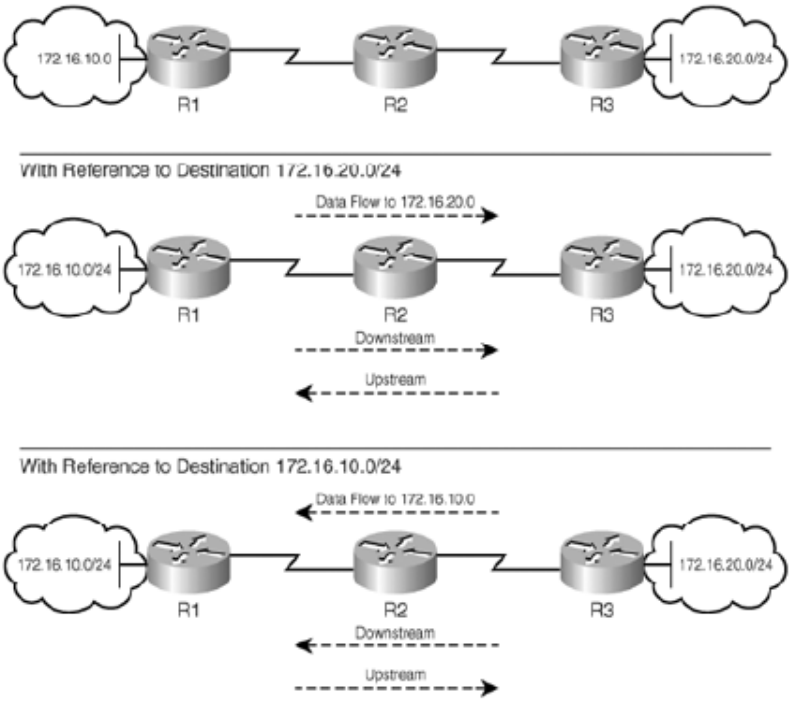
3. *MPLSEdge-Label Switch Router* (E-LSR) – sebuah LSR pada perbatasan domain *MPLS*. Ingress E-LSR bertugas dalam *label imposition* dan meneruskan paket melalui jaringan *MPLS-enabled*. Egress E-LSR bertugas dalam *label disposition* dan meneruskan paket *IP* ke tujuan.



Gambar 2.16 LSR dan E-LSR

(http://www.cisco.com/en/US/products/ps6557/prod_presentation_list.html)

4. *MPLS Label Switched Path* (LSP) – jalur pengiriman paket dari sumber ke tujuan pada jaringan *MPLS-enabled*
5. *Upstream and Downstream* – konsep dari *upstream* dan *downstream* merupakan poros untuk memahami operasi dari distribusi *label* (*control plane*) dan penerusan paket data dalam sebuah *domainMPLS*.



Gambar 2.17Upstream dan Downstream

(http://www.cisco.com/en/US/products/ps6557/prod_presentation_list.html)

2.2.5 *MPLS* Virtual Private Network (*MPLSVPN*)

Menurut Cisco Sistem Learning(2006), Teknologi *MPLS* sudah banyak diadopsi oleh para *Internetservice provider* (SP) bersamaan dengan teknologi *VPN* untuk menghubungkan antarcabang perusahaan. Di sini akan dijelaskan sedikit pondasi dan menunjukkan bagaimana cara untuk menyediakan layanan *VPN* ke pelanggan.

VPN pada umumnya digunakan oleh SP untuk menggunakan infrastruktur fisik dalam mengimplementasikan *point-to-pointlink* antar cabang perusahaan. Jaringan pelanggan yang diimplementasi dengan *VPN*akan berada pada pengawasan pelanggan yang disebut dengan *customer sites* yang terhubung

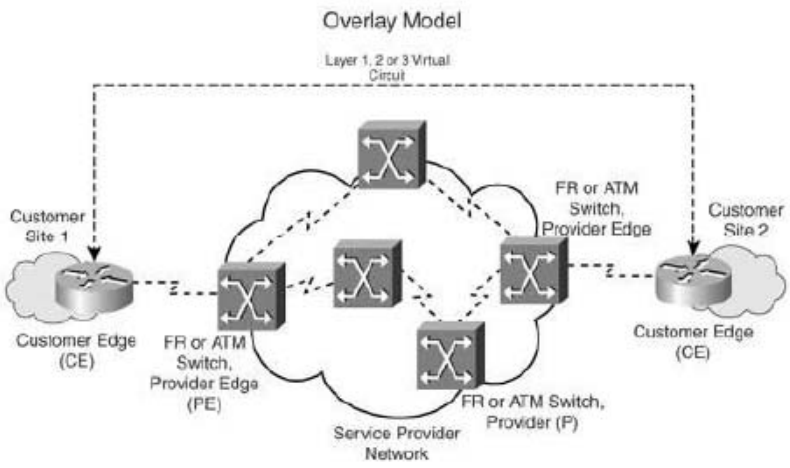
satu sama lain melalui jaringan SP. Biaya pengimplementasian tergantung pada jumlah *site* yang akan dihubungkan. (De Ghein, 2007, P213)

FrameRelay dan ATM merupakan teknologi pertama yang mengadopsi *VPN*. Pada umumnya, *VPN* terdiri dari 2 wilayah, yaitu :

1. Jaringan *customer*, terdiri dari *router-router* pada setiap *site* pelanggan yang disebut dengan *customer edge* (CE) router.
2. Jaringan *provider*, digunakan oleh SP untuk menawarkan *dedicated point-to-point links* melalui jaringannya. *Router* yang terhubung langsung dengan CE disebut dengan *provider edge* (PE) *router*. Selain itu juga terdapat *router* pada jaringan *backbone*-nya yang disebut dengan *provider* (P) *router*.

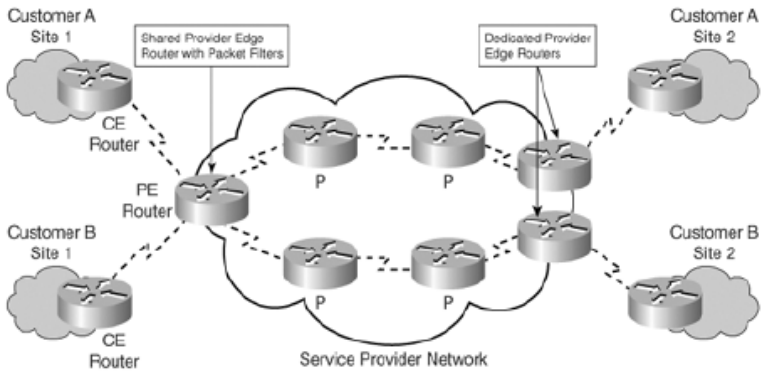
Berdasarkan partisipasi SP terhadap *routing* di pelanggan, implementasi *VPN* dapat dibagi menjadi:

1. *Overlay VPN* - Pada model ini *provider* menghubungkan antarcabang perusahaan dengan menggunakan jaringan pribadi yang *emulated*, SP tidak mencampuri proses *routing* di sisi pelanggan. SP hanya bertugas untuk menyediakan layanan data dengan menggunakan virtual *point-to-pointlink* yang dikenal dengan istilah *Layer 2 Virtual Circuit*.



Gambar 2.18 *OverlayVPN*

2. *Peer-to-Peer VPN* – Dikembangkan untuk mengatasi kelemahan pada model *Overlay* dan mengoptimalkan transportasi data melewati jaringan *backbone* SP. Oleh karena itu, SP juga ikut aktif dalam proses *routing* di sisi pelanggan.



Gambar 2.19 Peer to Peer *VPN*

2.2.6 Frame Relay

FrameRelay merupakan salah satu dari pengembangan dari teknologi paket *switching* yakin suatu teknologi WAN dan *cell circuit* pada ATM. Frame Relay juga merupakan satu protokol WAN yang bekerja pada transmisi paket data antar perangkat seperti DTE (Data Terminal Equipment) dengan DCE (Data Communication Equipment).

Inti dari Frame Relay adalah suatu transmisi paket diubah dalam bentuk frame yang masing-masing frame memiliki header paket dan payload. Seperti pada header IP , untuk frame header ditambahkan header Frame Relay pada IP. Akan tetapi berbeda dengan transmisi LAN, pada transmisi tidak menyertakan alamat IP tujuan dan sumber pada IP headernya.

Kekurangan dari Frame Relay adalah hilangnya kemampuan *flow-control* dan *error-control* jalur demi jalur dan kelebihannya Frame Relay proses komunikasi lebih ringan dan laju penyelesaian lebih cepat.

2.2.7 *Multiprotocol BGP* (*MP-BGP*)

Menurut Cisco Sistem Learning(2006), Protokol yang digunakan untuk menukar rute-rute *VPN*v4 adalah *multiprotocol BGP (MP-BGP). Router-router* PE harus menjalankan protokol *routing* IGP, yang pada saat ini Cisco mendukung *OSPF*v2 dan IS-IS pada jaringan *MPLS* SP. *MP-BGP* juga bertugas untuk memberi label *VPN*, serta memungkinkan penggunaan pengalamatan *VPN*v4 pada lingkungan*routerMPLSVPN* yang memungkinkan *overlapping* pengalamatan dengan beberapa pelanggan.

2.2.8*VPN* Security

Ada tiga hal dalam pengamanan IT dan juga berlaku dalam *VPN* yang harus selalu dimiliki :

1. Privacy (Confidentiality) : Data yang dikirimkan hanya dapat dibuka/diakses oleh yang berhak.
2. Reliability (Integrity) : Data yang dikirimkan tidak boleh mengalami perubahan dari pengirim data ke penerima data.
3. Availability : Data yang dikirimkan harus tersedia ketika dibutuhkan. Semua tujuan ini harus dicapai dengan menggunakan software, hardware, ISP, dan kebijakan keamanan yang tepat. Keamanan *VPN* itu sendiri dapat dicapai dengan menjaga lalu lintas (traffic), metode enkripsi yang kuat, teknik otentikasi yang aman, dan firewall yang mengatur traffic ke dan dari tunnel.

2.2.9 Teknologi *VPN*

VPN yang dibangun di *MPLS* berbeda dengan *VPN* lainnya seperti IPsec dan L2TP yang menggunakan tunneling dimana seakan-akan membuat jalur bawah tanah yang berfungsi sebagai jalur privasi antar router agar keamanan data terjaga saat terjadinya pengiriman packet. Berbeda dengan *MPLSVPN* yang dimana memaksa pemisahan lalu lintas dengan mentapkan tabel forwarding yang unik ke setiap customer.Pemisahan lalu lintas terjadi tanpa tunneling karena dibangun langsung ke jaringan.Keamanan jaringan *MPLSVPN* dibuat melalui kombinasi *MP-BGP* dengan resolusi alamat IP. Metode ini dapat memastikan bahwa *VPN* terisolasi dari satu sama lain. User hanya dapat berpatisipasi dalam intranet atau extranet jika mereka berada pada portal yang benar dan RD yang

tepat.Pengaturan ini membuat *MPLSVPN* hampir mustahil untuk di dimasuki dari luar maupun dalam yang bukan berada pada sitenya masing masing. Dalam *MPLS* ini menggunakan *VRF* untuk menghubungkan antara PE-PE nya serta untuk memisahkan site *VPN* yang mengarah ke CE, dengan cara traffic dipisahkan menggunakan label dan RD yang berbeda. *VRF* hanya bisa dibuat di router PE.